



Docket No.: 22040-00038-US1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Makoto Izawa et al.

Application No.: 10/710,987

Confirmation No.: 4986

Filed: August 16, 2004

Art Unit: N/A

For: CENTRAL ENCRYPTION MANAGEMENT
SYSTEM

Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

<u>Country</u>	<u>Application No.</u>	<u>Date</u>
Japan	2002-134681	May 9, 2002

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 22040-00038-US1 from which the undersigned is authorized to draw.

Dated: August 17, 2004
23552_1

Respectfully submitted,

By Larry J. Hume
Larry J. Hume

Registration No.: 44,163
CONNOLLY BOVE LODGE & HUTZ LLP
1990 M Street, N.W., Suite 800
Washington, DC 20036-3425
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application:

2002年 5月 9日

出願番号
Application Number:

特願2002-134681

ST. 10/C]:

[JP2002-134681]

願 人
Applicant(s):

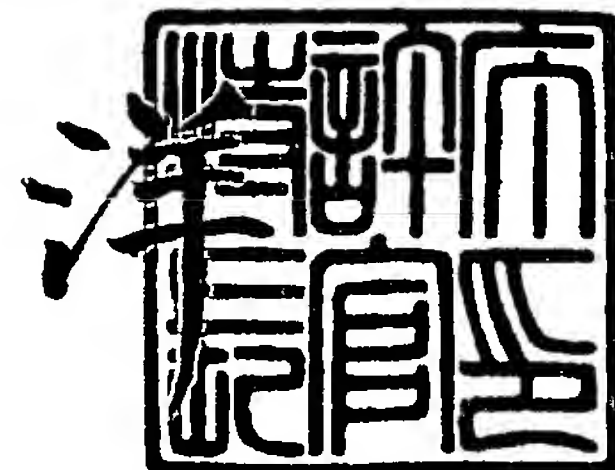
新潟精密株式会社
株式会社マイクロ総合研究所

CERTIFIED COPY OF
PRIORITY DOCUMENT

2004年 7月 5日

特許庁長官
Commissioner,
Japan Patent Office

小川



【書類名】 特許願

【整理番号】 14NS1431

【提出日】 平成14年 5月 9日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

【住所又は居所】 東京都品川区南品川 2 丁目 2 番 5 号 株式会社マイクロ
総合研究所内

【氏名】 井澤 誠

【発明者】

【住所又は居所】 東京都品川区南品川 2 丁目 2 番 5 号 株式会社マイクロ
総合研究所内

【氏名】 成田 宏光

【発明者】

【住所又は居所】 埼玉県上尾市緑丘 4 丁目 7 番 1 7 号

【氏名】 岡本 明

【特許出願人】

【識別番号】 591220850

【氏名又は名称】 新潟精密株式会社

【特許出願人】

【住所又は居所】 東京都品川区南品川 2 丁目 2 番 5 号

【氏名又は名称】 株式会社マイクロ総合研究所

【代理人】

【識別番号】 100105784

【弁理士】

【氏名又は名称】 橘 和之

【電話番号】 049-249-5122

【手数料の表示】

【予納台帳番号】 070162

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0006161

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化の一元集中管理システム

【特許請求の範囲】

【請求項 1】 暗号通信を行う複数の通信端末と、

上記複数の通信端末の間に接続され、暗号処理機能を有する通信端末との間で暗号化によるセキュリティを終端するためにデータの暗号化処理および復号化処理を行う暗号／復号手段を備えた暗号装置と、

上記暗号通信を行うのに必要な種々の情報の設定を、ネットワークを介して遠隔から上記通信端末および上記暗号装置に対して行うマネージャ端末とを備え、

上記複数の通信端末、上記マネージャ端末および上記暗号装置を有線または無線のネットワークにより接続して構成したことを特徴とする暗号化の一元集中管理システム。

【請求項 2】 上記暗号／復号手段は、上記暗号処理機能が導入された通信端末との間では暗号化されたデータの通信を行うとともに、上記暗号処理機能が導入されていない通信端末との間では暗号化されていないデータの通信を行うために上記暗号化処理および上記復号化処理を行うことを特徴とする請求項 1 に記載の暗号化の一元集中管理システム。

【請求項 3】 上記暗号装置は、一のポートより入力され上記暗号／復号手段により暗号化処理または復号化処理が施されたデータを、ルーティング処理をすることなく他のポートにそのまま出力するブリッジ手段を備えたことを特徴とする請求項 1 に記載の暗号化の一元集中管理システム。

【請求項 4】 暗号通信を行う複数の通信端末と、

上記複数の通信端末の間に接続され、一のポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行い、これにより得られたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力する暗号装置と、

上記暗号通信を行うのに必要な種々の情報の設定を、ネットワークを介して遠隔から上記通信端末および上記暗号装置に対して行うマネージャ端末とを備え、

上記複数の通信端末、上記マネージャ端末および上記暗号装置を有線または無線のネットワークにより接続して構成したことを特徴とする暗号化の一元集中管理システム。

【請求項 5】 上記暗号装置は、上記暗号化处理および上記復号化处理の制御に関して上記マネージャ端末から設定された情報を記憶する設定情報記憶手段を備え、

上記設定情報記憶手段に記憶されている設定情報と、上記一のポートより入力されたパケットに付加されているヘッダ情報とを照合して上記暗号化处理および上記復号化处理の制御を行うことを特徴とする請求項 1 または 4 に記載の暗号化の一元集中管理システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は暗号化の一元集中管理システムに関し、特に、ネットワーク上で外部から攻撃されることによる情報の盗聴や改ざん等のリスクを低減するために情報の暗号化／復号化を行うシステムに用いて好適なものである。

【 0 0 0 2 】

【従来の技術】

パーソナルコンピュータ（パソコン）をスタンドアロンで用いる場合は、パソコン内部の情報が盗み出されたり、改ざんされたり、破壊されたりする危険性は少ない。しかし、パソコンをインターネット等のネットワークに接続すると、やり取りされる情報は多くのネットワークをルーティングされていくことから、その途中において盗聴や改ざん等の行われる危険性が一気に増大する。

【 0 0 0 3 】

この問題を解決するための仕組みの 1 つとして、情報の暗号化がある。すなわち、送信側のパソコンで情報を暗号化して相手に送り、受信側のパソコンでこれを復号化して利用する。このようにすれば、ネットワークの途中で情報が盗聴されたとしても、情報が暗号化されているために、情報自体が見られる可能性が少なくなる。また、改ざんのリスクも低減される。

【 0 0 0 4 】**【発明が解決しようとする課題】**

しかしながら、暗号を利用するためには、暗号通信しようとする端末の全てに専用の暗号ソフトをインストールし、様々な設定をしなければならない。例えば、ある端末とある端末との間では暗号通信を行うが、他の端末との間では暗号通信を行わないなどといった暗号処理の有無、暗号通信を行う場合における暗号化のレベル、暗号化を行う時間帯、暗号鍵など、非常に多くの情報を個々の端末ごとに設定しなければならない。そのため、暗号を利用するためのシステムを構築するのに多大な労力を要するという問題があった。

【 0 0 0 5 】

本発明は、このような問題を解決するために成されたものであり、暗号を利用するために必要な各端末に対する様々な情報設定を簡単に行うことができるようにすることを目的とする。

【 0 0 0 6 】**【課題を解決するための手段】**

本発明の暗号化の一元集中管理システムは、暗号通信を行う複数の通信端末と、上記複数の通信端末の間に接続され、暗号処理機能を有する通信端末との間で暗号化によるセキュリティを終端するためにデータの暗号化処理および復号化処理を行う暗号／復号手段を備えた暗号装置と、上記暗号通信を行うのに必要な種々の情報の設定を、ネットワークを介して遠隔から上記通信端末および上記暗号装置に対して行うマネージャ端末とを備え、上記複数の通信端末、上記マネージャ端末および上記暗号装置を有線または無線のネットワークにより接続して構成したことを特徴とする。

【 0 0 0 7 】

本発明の他の態様では、上記暗号／復号手段は、上記暗号処理機能が導入された通信端末との間では暗号化されたデータの通信を行うとともに、上記暗号処理機能が導入されていない通信端末との間では暗号化されていないデータの通信を行うために上記暗号化処理および上記復号化処理を行うことを特徴とする。

【 0 0 0 8 】

本発明のその他の態様では、上記暗号装置は、一のポートより入力され上記暗号／復号手段により暗号化処理または復号化処理が施されたデータを、ルーティング処理をすることなく他のポートにそのまま出力するブリッジ手段を備えたことを特徴とする。

【 0 0 0 9 】

本発明のその他の態様では、暗号通信を行う複数の通信端末と、上記複数の通信端末の間に接続され、一のポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行い、これにより得られたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力する暗号装置と、上記暗号通信を行うのに必要な種々の情報の設定を、ネットワークを介して遠隔から上記通信端末および上記暗号装置に対して行うマネージャ端末とを備え、上記複数の通信端末、上記マネージャ端末および上記暗号装置を有線または無線のネットワークにより接続して構成したことを特徴とする。

【 0 0 1 0 】

本発明のその他の態様では、上記暗号装置は、上記暗号化処理および上記復号化処理の制御に関して上記マネージャ端末から設定された情報を記憶する設定情報記憶手段を備え、上記設定情報記憶手段に記憶されている設定情報と、上記一のポートより入力されたパケットに付加されているヘッダ情報とを照合して上記暗号化処理および上記復号化処理の制御を行うことを特徴とする。

【 0 0 1 1 】

【発明の実施の形態】

以下、本発明の一実施形態を図面に基づいて説明する。

図 1 は、本実施形態による暗号化の一元集中管理システムの全体構成例を示す図である。

【 0 0 1 2 】

図 1 において、1 は暗号装置であり、2 つのポートを有し、一方のポートにはネットワークプリンタ 2、DB サーバ 3、ネットワークターミナル 4 などのデバイスが接続され、他方のポートにはハブ 5 が接続されている。この暗号装置 1 は

、ネットワークプリンタ 2、DBサーバ 3、ネットワークターミナル 4 などのデバイスと、ハブ 5 との間でデータの中継を行う。

【0 0 1 3】

ネットワークプリンタ 2 は、暗号ソフトを物理的にインストールできない端末である。DBサーバ 3 は、動作安定上等の問題から余分な暗号ソフトをインストールすることが好ましくない端末である。ネットワークターミナル 4 は、OS（オペレーティングシステム）がなく暗号ソフトを動作させることができない端末である。したがって、これらの端末 2～4 には暗号ソフトはインストールされていないものとする。

【0 0 1 4】

また、ハブ 5 は、物理層においてデータの中継する機器であり、上述した暗号装置 1 の他に、無線通信用のアクセスポイント 6、デスクトップパソコン 7、暗号化／復号化に関する種々の情報設定を行うためのマネージャ端末 1 2 が接続されている。この場合のハブ 5 は、暗号装置 1 と、アクセスポイント 6 およびデスクトップパソコン 7 との間で暗号通信のためのデータ中継を行う。また、マネージャ端末 1 2 と、その他の暗号装置 1、アクセスポイント 6 およびデスクトップパソコン 7 との間で各種情報設定のためのデータ中継も行う。

【0 0 1 5】

さらに、上記アクセスポイント 6 には、デスクトップパソコン 8 とラップトップパソコン 9 とが無線により接続されている。デスクトップパソコン 7、8 およびラップトップパソコン 9 には、データの暗号化および復号化を行うための暗号ソフトがインストール可能であり、実際に、暗号／復号処理を行うためのエージェントソフトがインストールされているものとする。暗号装置 1 にも、これと同様の暗号エージェントソフトがインストールされている。

【0 0 1 6】

このような構成により、暗号ソフトがインストールされていないネットワークプリンタ 2、DBサーバ 3 およびネットワークターミナル 4 と、暗号ソフトがインストールされているパソコン 7～9（これらのデバイス 2～4，7～9 は何れも本発明の通信端末に相当）との間で、暗号装置 1、ハブ 5 およびアクセスポイ

ント 6 を介してデータ通信が行われる。

【 0 0 1 7 】

その際、暗号装置 1 は、暗号ソフトがインストールされているパソコン 7 ～ 9 との間では暗号化されたデータの通信を行うとともに、暗号ソフトがインストールされていない端末 2 ～ 4 との間では暗号化されていないデータの通信を行うために暗号化処理および暗号の復号化処理を行う。

【 0 0 1 8 】

例えば、デスクトップパソコン 7 からネットワークプリンタ 2 にデータを送出してプリントアウトするときは、まずデスクトップパソコン 7 にインストールされている暗号ソフトを用いてデータを暗号化し、ハブ 5 を介して暗号装置 1 に供給する。次に暗号装置 1 は、受け取ったデータを復号化し、ネットワークプリンタ 2 に送出する。

【 0 0 1 9 】

また、例えば DB サーバ 3 にて管理されているデータをラップトップパソコン 9 に取り込むときは、DB サーバ 3 は、与えられる要求に応じて該当するデータを暗号装置 1 に供給する。この暗号化されていないデータを受け取った暗号装置 1 は、そのデータを暗号化し、ハブ 5 およびアクセスポイント 6 を介してラップトップパソコン 9 に送信する。ラップトップパソコン 9 は、受け取ったデータを復号化し、所望の処理に利用する。

【 0 0 2 0 】

以上の説明から明らかなように、暗号装置 1 を用いることによって、専用の暗号ソフトをインストールできない端末 2 ～ 4 を有する企業内 LAN (Local Area Network) の中でも、暗号を利用することが可能となる。これにより、外部からの不正侵入や攻撃によって LAN 内部の機密情報が盗まれたり改ざんされたりする危険性が少ないセキュアなネットワーク 10 を構築することができる。

【 0 0 2 1 】

なお、暗号装置 1 と各端末 2 ～ 4 との間において暗号は利用できないが、これらを繋ぐケーブル 11 は物理的に短い配線であり、この部分が外部アタックされることによって盗聴や改ざんが行われる可能性は極めて低いので、セキュリティ

上で特に問題となることはない。

【 0 0 2 2 】

上記のような暗号システムにおいて、暗号装置 1 および各パソコン 7 ～ 9 が備える暗号エージェントソフトに対して設定すべき種々の情報、例えば、暗号／復号処理の有無、ある端末とある端末との間ではパケットを破棄するなどといった通信の可否、暗号化のレベル、暗号化を行う時間帯、部門毎の暗号ポリシー、暗号鍵などの情報は、マネージャ端末 1 2 からハブ 5 を介して暗号装置 1 および各パソコン 7 ～ 9 に必要な情報をダウンロードして設定する。

【 0 0 2 3 】

これにより、暗号の利用に必要な種々の情報を端末ごとに個別に設定する必要がなくなり、マネージャ端末 1 2 から暗号システムの全体を一元的に集中して管理することができる。したがって、各端末に対する様々な情報設定を簡単に行うことができ、暗号システムの構築およびその後のメンテナンスにかかる労力を大幅に削減することができる。

【 0 0 2 4 】

従来、プリンタやファクシミリなど物理的に暗号ソフトをインストールできない端末や、プリントサーバやデータベースサーバなど余分なソフトをインストールすることが好ましくない端末、OS がなく単なるネットワークターミナルとして機能する端末などを備えた企業内 LAN の中では、暗号ソフトを実質的にインストールできないため、暗号を利用することは難しかった。

【 0 0 2 5 】

そのため、従来の暗号システムは、インターネットに接続された端末どうしがやり取りする情報を途中のインターネット上において暗号化するものであった。この場合、暗号通信する端末はインターネット上に多数散在しているため、これら多数の端末について暗号化の一元集中管理をすることは非常に困難であった。これに対して、本実施形態によれば、企業内 LAN の中で暗号を利用することができるようにしているので、その LAN 内で終端された暗号化を一元的に管理することが可能となる。

【 0 0 2 6 】

図 2 は、本実施形態による暗号化の一元集中管理システムの他の構成例を示す図である。なお、この図 2 において、図 1 に示した構成要素と同一の機能を有する構成要素には同一の符号を付している。図 2 において、暗号装置 1 は、一方のポートにインターネット 2 0 が接続され、他方のポートにハブ 5 が接続されている。インターネット 2 0 の先には、図 1 に示したネットワークプリンタ 2、DB サーバ 3、ネットワークターミナル 4 などのように暗号ソフトをインストールできない端末、あるいは、パソコン 7～9 のように暗号ソフトがインストールされた端末が複数台接続されている。

【 0 0 2 7 】

図 1 に示した例では、1 台の暗号装置 1 に対して 1 台のデバイスが接続されており、1 台のデバイスに関する暗号／復号処理を 1 台の暗号装置 1 が専用で行っていた。すなわち、図 1 に示す暗号装置 1 は、暗号ソフトがインストールされたパソコン 7～9 と、暗号ソフトがインストールされていない 1 台のデバイスとの間に接続され、暗号ソフトがインストールされたパソコン 7～9 との間で暗号化によるセキュリティを終端していた。

【 0 0 2 8 】

これに対して、図 2 に示す例では、暗号装置 1 は、暗号ソフトがインストールされたパソコン 7～9 と、インターネット 2 0 に接続された複数台のデバイスとの間に接続されている。このように、暗号装置 1 は、複数台のデバイスに対して暗号化によるセキュリティを終端することも可能である。この場合、暗号装置 1 は、接続されているデバイスの数だけデータパスを有し、それぞれのデバイス毎に異なる暗号鍵で暗号／復号処理を行う。

【 0 0 2 9 】

上記複数台のデバイスは、暗号ソフトがインストールされていても良いし、インストールされていなくても良い。暗号ソフトがインストールされている場合には、セキュアネットワーク 1 0 の外部にあるインターネット 2 0 上でも暗号を利用することができる。なお、上記複数台のデバイスは、インターネット 2 0 を介して接続されている必要は必ずしもなく、暗号装置 1 に直接接続しても良い。この場合、暗号装置 1 は 2 つ以上のポートを有することになる。

【0 0 3 0】

図 3 は、本実施形態による暗号化の一元集中管理システムの更に別の構成例を示す図である。なお、この図 3 において、図 1 に示した構成要素と同一の機能を有する構成要素には同一の符号を付している。図 3 に示す例も図 2 の例と同様に、1 台の暗号装置 1 が複数台のデバイスに対して暗号化によるセキュリティを終端する例である。

【0 0 3 1】

図 3 に示す例では、セキュアネットワーク 1 0 の内部は、3 台のパソコン 7 ～ 9 が全てアクセスポイント 6 _1 に無線 LAN にて接続されている。アクセスポイント 6 _1 は、暗号装置 1 を介してインターネット 2 0 に接続されている。また、複数のアクセスポイント 6 _1, 6 _2 を備え、1 台のアクセスポイント 6 _1 でカバーしきれない通信範囲を他のアクセスポイント 6 _2 がカバーすることにより、比較的広域な無線 LAN 環境を提供している。暗号装置 1 は、アクセスポイント 6 _1, 6 _2 毎に個別に接続されている。

【0 0 3 2】

このように構成された暗号システムにおいて、例えば一方のアクセスポイント 6 _1 に接続されているラップトップパソコン 9 がその通信可能範囲を超えて移動したときには、他方のアクセスポイント 6 _2 に切り替えて通信を継続するローミングを行うことができる。しかも、上述したように、暗号通信を行うパスの設定をマネージャ端末 1 2 により一元管理しているので、複数のアクセスポイント 6 _1, 6 _2 間でローミングを行っても、暗号通信を継続して行うことができる。

【0 0 3 3】

また、この図 3 に示す例においてマネージャ端末 1 2 は、インターネット 2 0 に接続されている。この場合のマネージャ端末 1 2 は、暗号エージェントソフトに対して設定すべき種々の情報を、インターネット 2 0 を介して暗号装置 1 および各パソコン 7 ～ 9 にダウンロードして設定する。

【0 0 3 4】

なお、上記図 1 ～ 図 3 においては、1 つのセキュアネットワーク 1 0 とその中の暗号化を一元管理する 1 つのマネージャ端末 1 2 とを備える例について説明し

ている。これに対し、複数のセキュアネットワーク 1 0 とその中の暗号化をそれぞれ一元管理する複数のマネージャ端末 1 2 とを備え、各マネージャ端末 1 2 がインターネット 2 0 等を介して互いにデータ通信をして暗号化／復号化に関する種々の情報を適宜設定するようにすることにより、複数のセキュアネットワーク 1 0 をまとめて全体として 1 つの暗号システムを構築することも可能である。

【 0 0 3 5 】

図 4 は、図 1 に示した暗号システムにおいて、暗号装置 1 およびこれに直接および間接的に接続される DB サーバ 3 およびラップトップパソコン 9 におけるプロトコルの階層構造を示す図である。図 4 に示す例では、DB サーバ 3 には暗号ソフトがインストールされておらず（I P - S e c がない）、ラップトップパソコン 9 には暗号ソフトがインストールされている（I P - S e c を有する）。この DB サーバ 3 およびラップトップパソコン 9 の間に、本実施形態の暗号装置 1 が接続されている。ここでは、DB サーバ 3 にて保存されているデータを暗号装置 1 に送り、ここでデータを暗号化してパソコン 9 に送るような利用形態を想定している。

【 0 0 3 6 】

図 4 に示すように、DB サーバ 3 およびパソコン 9 はそれぞれ 1 つのポート 3 1, 3 2 を有し、その中継機となる暗号装置 1 は 2 つのポート 3 3, 3 4 を有している。暗号装置 1 の各ポート 3 3, 3 4 に対して物理層および M A C 層（データリンク層）が個別に設けられ、各ポート 3 3, 3 4 に共通なものとして I P - S e c（暗号／復号処理機能）、I P 層（ネットワーク層）および T C P / U D P 層（トランスポート層）が設けられている。

【 0 0 3 7 】

層が深くなるほどユーザからは遠くなり、逆に層が浅くなるほどユーザに近くなる。DB サーバ 3 およびパソコン 9 の I P 層よりも上位層には、T C P / U D P 層およびアプリケーション層（共に図示せず）が存在し、ユーザが使用するアプリケーションと下の層との橋渡しが行われる。

【 0 0 3 8 】

データの送信側では、上位層から下位層に向かって各層を通過するごとにデー

タが変換されるとともに、それぞれの層間でデータ伝送を可能にするためのヘッダが付加されていく。逆に、データの受信側では、各層宛てのヘッダを参照して各層で必要なデータが抽出される。そして、抽出されたデータは上位層へ引き渡され、最終的にアプリケーション層を介してユーザに届けられる。

【 0 0 3 9 】

以下に、それぞれの層の機能について説明する。TCP/UDP層は、データを渡すべきアプリケーションの特定や、パケットの状態の管理などを行うレイヤである。データ送信側においては、上位層（アプリケーション層）から渡されたデータを相手のどのアプリケーションに渡すべきかを認識し、宛先ポート番号をデータに付加して下位層（ネットワーク層）に渡す。一方、データ受信側においては、下位層から渡されたパケットについて、通信の状態等によって抜けが生じていないかどうかを監視する。

【 0 0 4 0 】

IP層は、複数のネットワークにまたがった端末間のデータ転送あるいはデータ中継に関する取り決めや制御を行うためのレイヤである。通信相手となる送信側のDBサーバ3と受信側のパソコン9にはそれぞれ異なるIPアドレス①、④が割り振られており、これらを明確にすることによって、end to endによる論理的な通信経路が決定する。

【 0 0 4 1 】

MAC（Media Access Control）層は、隣接機器のノード間で信頼性の高いデータ伝送を保証するためのレイヤであり、製造段階で各機器に割り当てられた物理的なMACアドレスを有する。データ送信側においては、IP層で通信相手のIPアドレスが明確になると、その下位に位置するMAC層において、確立された相手のIPアドレスをもとに、経由する次の機器（物理的に接続されている隣接ノード）の宛先を決定する。一方、データ受信側においては、MACアドレスをもとに自分宛のパケットであることを認識した後、その上位層のIP層でIPアドレスを解析し、そのパケットを他の機器に対して更にルーティングするか自分に取り込むかを判断する。

【 0 0 4 2 】

物理層は、上位層から渡されたデータを電気信号や光信号に変換し、同軸ケーブルや光ファイバケーブル等の伝送媒体を介して実際のデータ伝送を行ったり、伝送媒体から送られてきた電気信号や光信号を上位層で認識可能なデータに変換し、それを上位層に渡したりするためのレイヤである。物理層の上位層である M A C 層では、物理層の通信インタフェースに依存した手法に従って上述の処理を行う。

【 0 0 4 3 】

I P - S e c は、データの暗号化処理および復号化処理を行う機能部である。すなわち、M A C 層から渡されたデータを取得して、当該データの暗号化処理および暗号の復号化処理を行う。

【 0 0 4 4 】

本実施形態の暗号装置 1 は、I P - S e c により 2 つのポート 3 3, 3 4 間をブリッジさせているところに特徴がある。すなわち、本実施形態の暗号装置 1 では、D B サーバ 3 とパソコン 9 との間におけるデータ転送に関しては I P 層および T C P / U D P 層は用いず、I P 層よりも下位層で処理を行う。具体的には、第 1 のポート 3 3 より入力されたデータに対して I P - S e c で暗号化処理を行い、それにより得られたデータを、I P 層にてルーティングすることなく（I P 層に渡すことなく）他方のポートにそのまま渡して出力する。

【 0 0 4 5 】

すなわち、D B サーバ 3 にて作成されたパケットデータは、当該 D B サーバ 3 の M A C 層、物理層を通過して送信され、暗号装置 1 の第 1 のポート 3 3 より受信される。受信されたパケットデータは物理層、M A C 層を通過して I P - S e c に渡され、ここで暗号化処理が行われる。この暗号化されたパケットデータは、M A C 層および物理層を通過して第 2 のポート 3 4 より送信される。

【 0 0 4 6 】

第 2 のポート 3 4 より送信されたパケットデータは、パソコン 9 で受信され、物理層、M A C 層を通過して I P - S e c に渡されて、暗号が復号化される。そして、復号化されたデータが I P 層を通過して図示しないアプリケーション層に渡される。これにより、D B サーバ 3 が暗号ソフトを備えていなくても、パソコン 9

に対して暗号化されたデータを送信することが可能となる。

【0 0 4 7】

なお、暗号装置 1 の I P 層および T C P / U D P 層は、上述したマネージャ端末 1 2 から暗号装置 1 自身に暗号化／復号化に関する各種の情報を設定する際に利用される。この種の設定情報は、I P - S e c ブリッジの機能によってメモリ上に保持される。I P - S e c は、当該メモリに保持されている設定情報と、ポート 3 3, 3 4 より入力されたパケットに付加されているヘッダ情報（例えば、送信元 I P アドレスおよび宛先 I P アドレス）とを照合して、暗号／復号処理の制御などを行う。

【0 0 4 8】

このように、本実施形態の暗号装置 1 では、一のポートから入力されたデータを I P - S e c で暗号化／復号化し、これにより得られたデータを I P 層に渡すことなく、ルーティング処理をせずにそのまま他のポートに転送するようにしているので、データ通信時に暗号装置 1 の I P アドレスを不要とすることができる。すなわち、I P アドレスを持たずに I P 層の暗号／復号処理を行うことが可能である。そのため、暗号装置 1 自身に対する煩雑な I P アドレス設定の必要をなくすることができる。

【0 0 4 9】

また、暗号装置 1 の両側に接続される端末は同じネットワークに属することになり、暗号装置 1 の入力ポートと出力ポートとで I P アドレスが変わることがなくなる。これにより、暗号装置 1 のネットワーク上における接続の有無に関わりなく、I P アドレスの透過性を保つことができる。すなわち、ネットワーク上に暗号装置 1 を接続したり、ネットワーク上から暗号装置 1 を外したりする際に、当該暗号装置 1 に接続される端末のアドレス設定も変更する必要がない。

【0 0 5 0】

例えば、図 4 のように D B サーバ 3 とパソコン 9 との間に暗号装置 1 を挿入した場合も、暗号装置 1 を挿入せずに D B サーバ 3 とパソコン 9 との間で直接通信を行う場合も、D B サーバ 3 とパソコン 9 との間を流れるパケットの I P アドレスは、図 5 に示す通りのままで不変である。したがって、暗号装置 1 の接続の有

無によってアドレス設定を何ら変更する必要がない。

【 0 0 5 1 】

これにより、ネットワークシステムの導入時やメンテナンス時には、本実施形態の暗号装置 1 を適当な箇所にただ挿入したり、あるいはただ取り外したりするだけ良くなり、煩雑なアドレス設定は行わないので、作業負荷を大幅に削減することができる。

【 0 0 5 2 】

さらに、本実施形態の場合、MAC アドレスについても透過性を保つことができる。図 6 は、DB サーバ 3 からパソコン 9 にデータを送り、その間の暗号装置 1 でデータを暗号化する場合におけるパケットを示す図である。図 6 (a) は第 1 のポート 3 3 にて受信するパケットを示し、図 6 (b) は第 2 のポート 3 4 より送信するパケットを示す。なお、IP - Sec には、データ部のみを暗号化するトランスポートモードと、パケット全てを暗号化して更に新しいヘッダを追加するトンネルモードとがある。送信パケットに関しては、これら 2 つのモードについてそれぞれ示している。

【 0 0 5 3 】

また、図 7 は、本実施形態との比較のために、従来の VPN ルータを用いたシステムにおいて一方のパソコンから他方のパソコンにデータを送り、その間の VPN ルータでデータを暗号化する場合におけるパケットを示す図である。図 7 (a) は VPN ルータの第 1 のポートにて受信するパケットを示し、図 7 (b) は第 2 のポートより送信するパケットを示す。この図 7 においても、送信パケットに関しては、2 つのモードについてそれぞれ示している。

【 0 0 5 4 】

図 6 から明らかなように、本実施形態によれば、IP アドレスだけでなく、MAC アドレスについても第 1 のポート 3 3 と第 2 のポート 3 4 とで異なることなく、MAC アドレスの透過性を保つことができる。すなわち、本実施形態の暗号装置 1 は、IP - Sec を有してデータの暗号／復号処理を行うことを除けば、一方のポートから入力されたデータを他方のポートにただ流すだけなので、データ通信時には MAC アドレスも不要とすることができる。

【 0 0 5 5 】

なお、以上に説明した実施形態は、本発明を実施するにあたっての具体化の一例を示したものに過ぎず、これによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【 0 0 5 6 】**【発明の効果】**

本発明は上述したように、例えば暗号処理機能が導入された端末との間で暗号化によるセキュリティを終端するために暗号化処理および暗号の復号化処理を行う暗号／復号手段を備えて暗号装置を構成し、この暗号装置と、暗号通信を行う複数の通信端末と、暗号通信を行うために必要な種々の情報の設定を遠隔から通信端末および暗号装置に対して行うマネージャ端末とを接続して暗号システムを構成するようにしたので、専用の暗号ソフトをインストールできない端末を有する企業内 LAN の中でも暗号を利用することができるようになり、その LAN 内で終端された暗号化をマネージャ端末において一元的に集中管理することが可能となる。これにより、暗号システムの構築およびその後のメンテナンスにかかる労力を大幅に削減することができる。

【図面の簡単な説明】**【図 1】**

本実施形態による暗号化の一元集中管理システムの構成例を示す図である。

【図 2】

本実施形態による暗号化の一元集中管理システムの他の構成例を示す図である。

【図 3】

本実施形態による暗号化の一元集中管理システムの更に別の構成例を示す図である。

【図 4】

本実施形態による暗号装置およびこれに接続される DB サーバおよびパソコンにおけるプロトコルの階層構造を示す図である。

【図 5】

本実施形態においてネットワーク上を流れるパケットの I P アドレスについて説明するための図である。

【図 6】

本実施形態の暗号装置を流れるパケットの M A C アドレスについて説明するための図である。

【図 7】

従来の V P N ルータを流れるパケットの M A C アドレスについて説明するための図である。

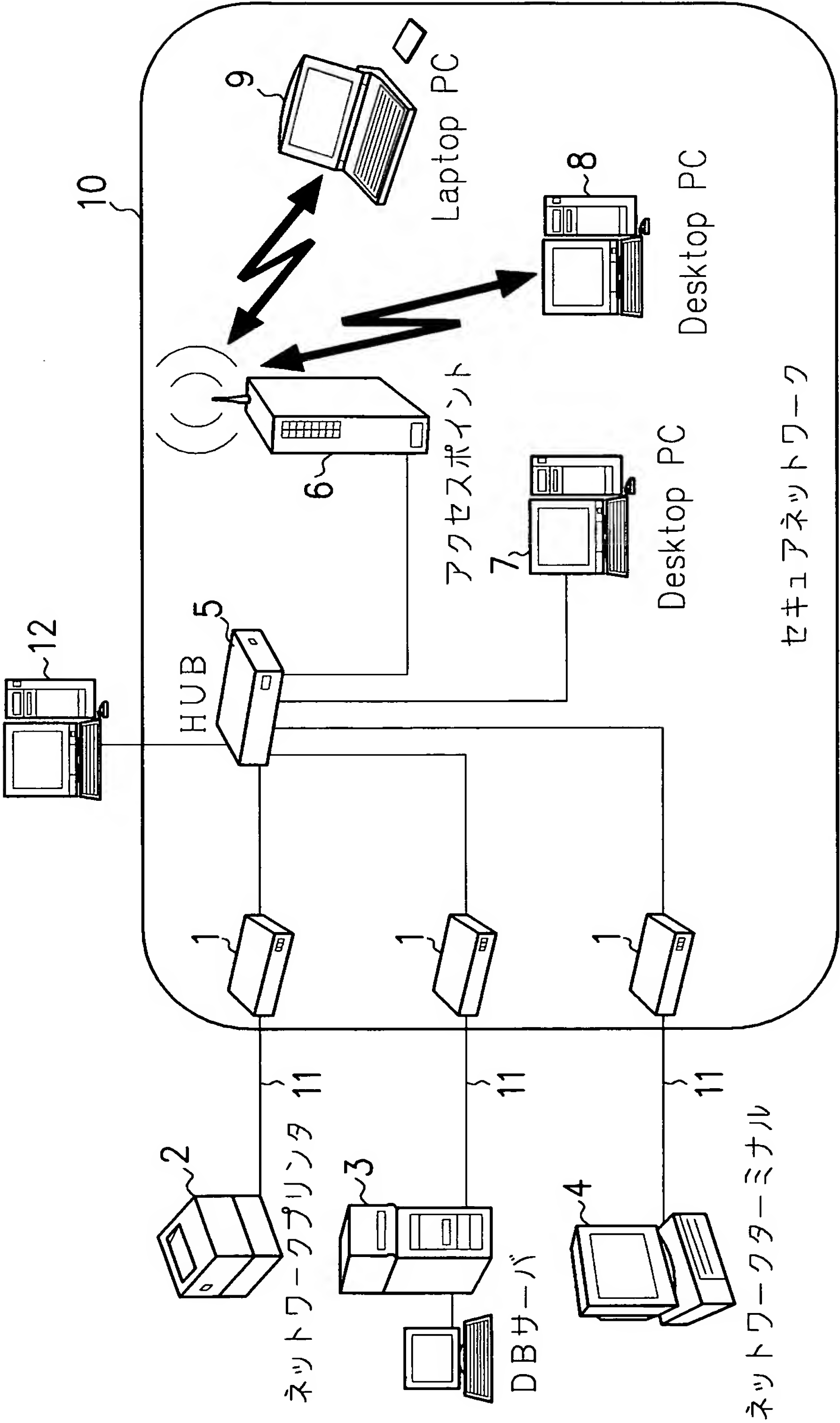
【符号の説明】

- 1 暗号装置
- 2 ネットワークプリンタ
- 3 D B サーバ
- 4 ネットワークターミナル
- 5 ハブ
- 6 アクセスポイント
- 7, 8 デスクトップパソコン
- 9 ラップトップパソコン
- 1 0 セキュアネットワーク
- 1 1 ケーブル
- 1 2 マネージャ端末
- 2 0 インターネット

【書類名】 図面

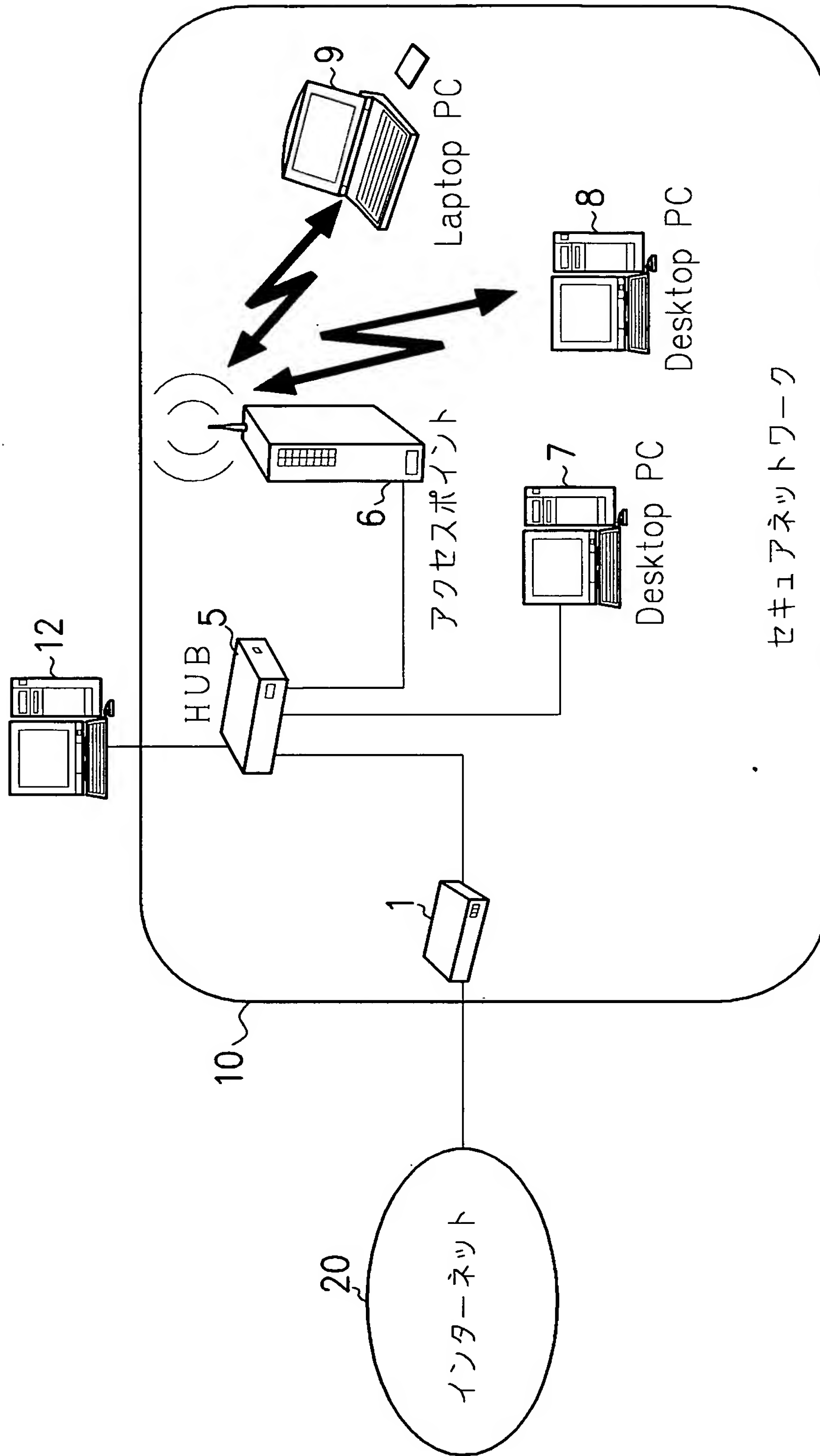
【図 1】

本実施形態による暗号システムの構成例



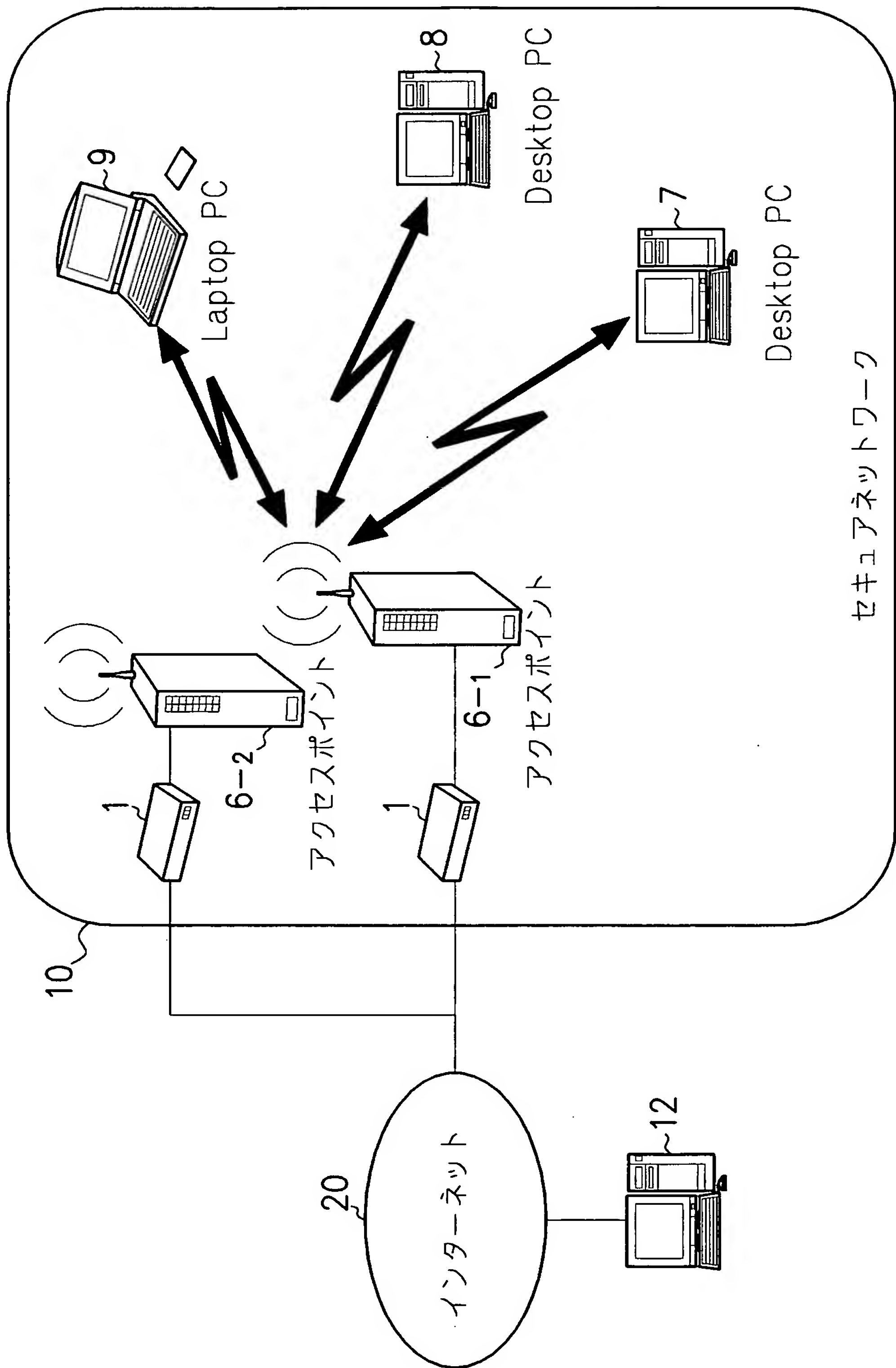
【図 2】

本実施形態による暗号システムの他の構成例



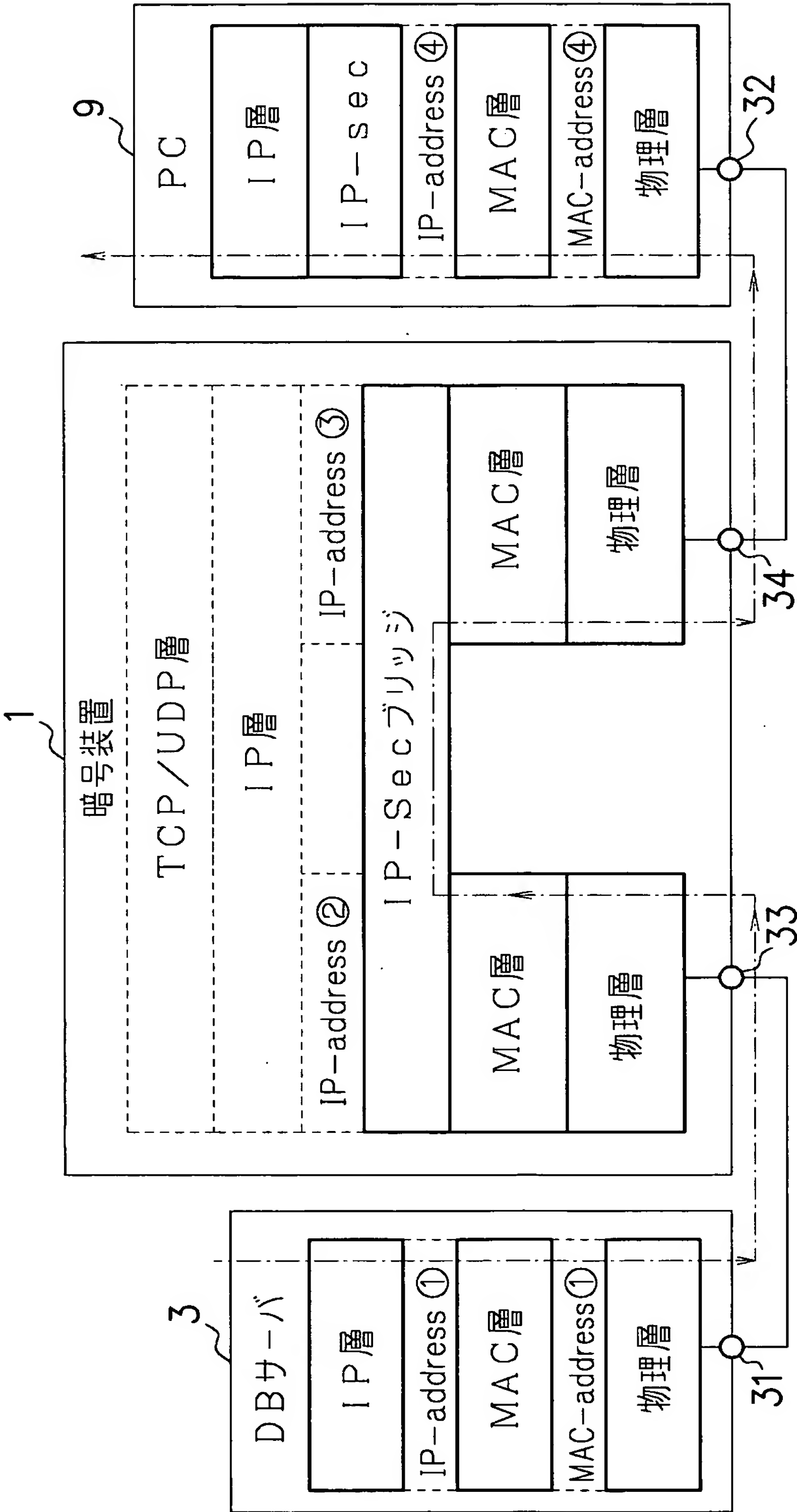
【図 3】

本実施形態による暗号システムの他の構成例



【図 4】

本実施形態による暗号装置のレイヤ構造



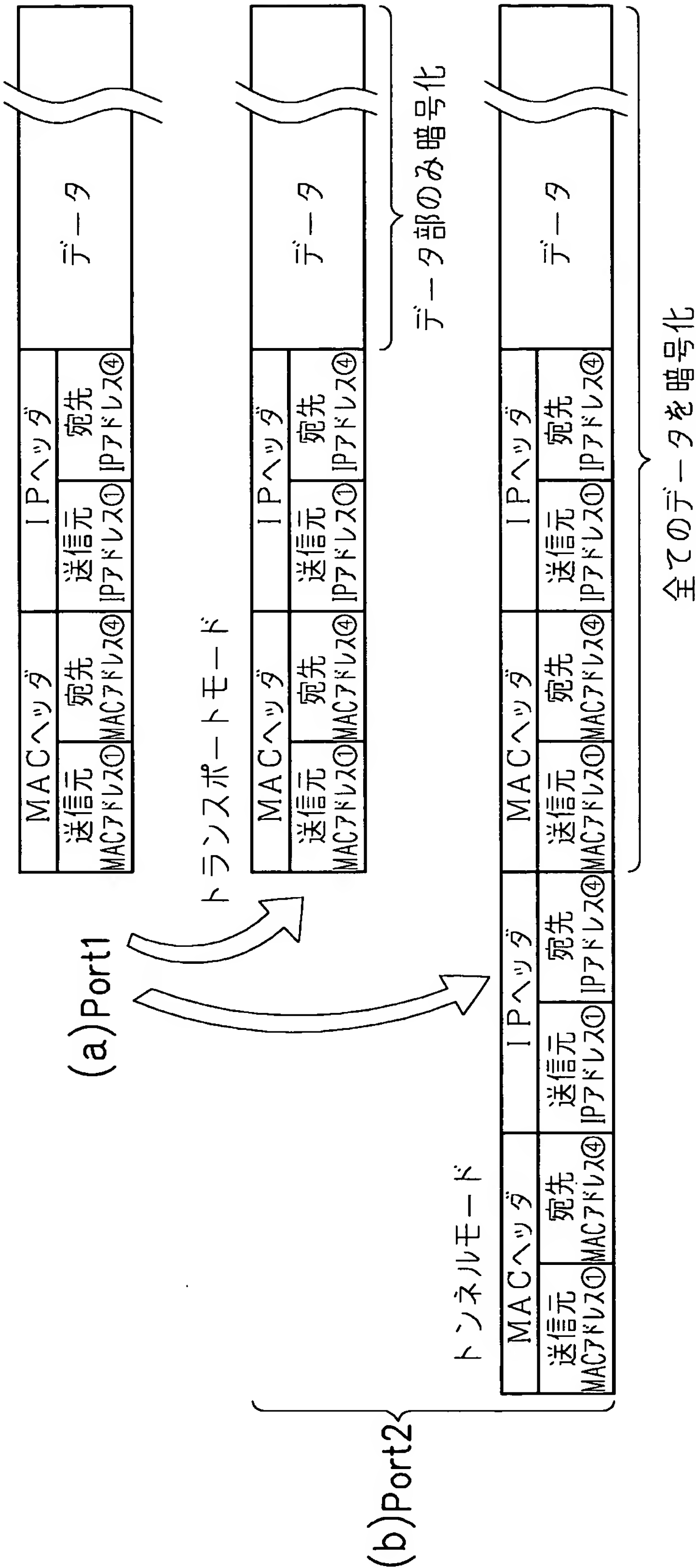
【図 5】

本実施形態のパケット

送信元 IP アドレス①		宛先 IP アドレス④		データ
ネットワークアドレス	ホストアドレス	ネットワークアドレス	ホストアドレス	
ネットワーク A	XXXXXXXX	ネットワーク A	XXXXXXXX	

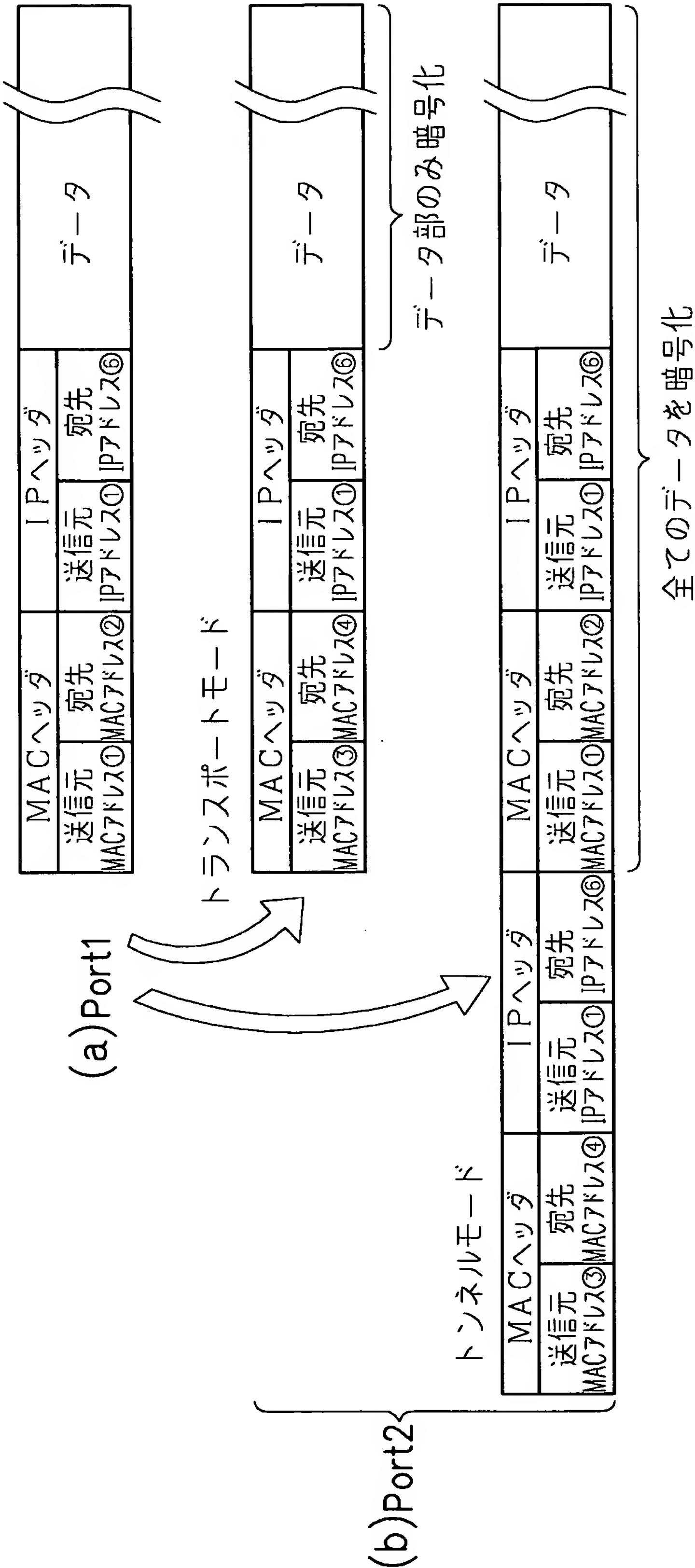
【図 6】

本実施形態の暗号装置によるパケット



【図 7】

従来のVPNルータによるパケット



【書類名】 要約書

【要約】

【課題】 暗号を利用するために必要な各端末に対する様々な情報設定を簡単に行うことができるようにする。

【解決手段】 暗号処理機能が導入された端末との間で暗号化によるセキュリティを終端するために暗号化処理および暗号の復号化処理を行う暗号／復号手段を備えて暗号装置 1 を構成し、この暗号装置 1 と、暗号通信を行う複数の通信端末 2 ～ 9 と、暗号通信に必要な種々の情報の設定を遠隔から通信端末 7 ～ 9 および暗号装置 1 に対して行うマネージャ端末 1 2 とを接続して暗号システムを構成することにより、専用の暗号ソフトをインストールできない端末を有する企業内 LAN の中でも暗号を利用することができるようにして、その LAN 内で終端された暗号化をマネージャ端末 1 2 において一元的に集中管理することができるようにする。

【選択図】 図 1

特願 2 0 0 2 - 1 3 4 6 8 1

出 願 人 履 歴 情 報

識別番号 [5 9 1 2 2 0 8 5 0]

1. 変更年月日	1 9 9 6 年 5 月 9 日
[変更理由]	住所変更
住 所	新潟県上越市西城町 2 丁目 5 番 1 3 号
氏 名	新潟精密株式会社

特願 2 0 0 2 - 1 3 4 6 8 1

出 願 人 履 歴 情 報

識別番号 [5 0 1 3 0 6 9 7 7]

1 . 変更年月日 2 0 0 1 年 8 月 2 日
[変更理由] 新規登録
住 所 東京都品川区南品川 2 丁目 2 番 5 号
氏 名 株式会社マイクロ総合研究所